Применета информатика
Стручен текст

УДК: 004.7.056:004.63
Professional paper

м-р Наташа МАКСИМОВА
м-р Влатко Т. ЈОВАНОВСКИ
м-р Лимонка ЛАЗАРОВА

M.Sc., Nataša MAKSIMOVA
M.Sc., Vlatko T. JOVANOVSKI
M.Sc., Limonka LAZAROVA

КОМПЈУТЕРСКА И МРЕЖНА БЕЗБЕДНОСТ НА СИСТЕМИ ЗА УПРАВУВАЊЕ СО ДОКУМЕНТИ

Апстракт: Безбедноста на податоците и заштитата на мрежите е од големо значење за управување со документи во правосудството, министерствата и другите владини институции. Затоа, во трудот се разгледани техники за криптирање на податоци. Даден е краток опис за криптографија со приватен клуч и криптографија со јавен клуч. Се задржуваме на RSA алгоритамот, како еден од најсигурните алгоритами со јавни клучеви. Исто така, ги објаснуваме дигиталните сертификати кои се користат за заштита и електронски пренос на податоци.

Клучни зборови: *безбедност, криптографија, приватен клуч, јавен клуч, RSA алгоритам и дигитален сертификат.*

Abstract: Data security and the protection of networks are very important for managing documents in the justice, ministries and other government institutions. In this paper are considered techniques for data encryption. A simple description is given for cryptography with private key and cryptography with public key. We have dwelled on the RSA algorithm as one of the most secure public key and we have explained the digital certificates which are used for security and electronic data transmission.

Keywords: *security, cryptography, private key, public key, RSA algorithm, digital certificate.*

Вовед

Компјутерската безбедност на електронските податоци е сериозна работа. Со зголемување на бројот на компании и државни институции кои работат во мрежа или преку Интернет се наметнува прашањето за **безбедност**. Корисниците на услугите внесуваат доверливи информации, се врши размена на документи, се испраќаат податоци и материјали до институциите по електронски пат. Во исто време се зголемува бројот на хакерски напади и оштетување или уништување на податоци на компании и владиниот сектор поврзани на Интернет. Еден начин за обезбедување на безбедни трансакции е со криптирање или шифрирање на податоци, со

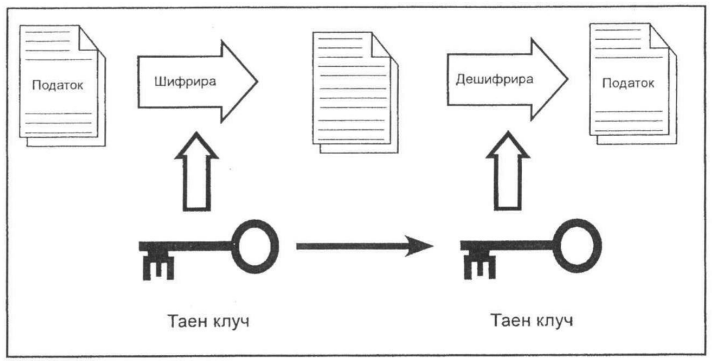
информациите ќе бидат прочитани само од тие за кои се наменети.
ата која се занимава со трансформација на информации (кои се
т - текст) во информации кои не може да бидат прочитани се нарекува
ографија. Во овој процес информацијата се шифрира за да не може
е прочитана или изменета од никого освен од примачот.
лавната цел на трудот е да опише воспоставување на систем за
та на веќе интегриран државен информационен систем за управување
ументи, кој треба да ги вклучи сите релевантни институции и треба
овозможи на органите да ги автоматизираат работните процеси, со
се овозможи следење на текот на документација во процесот на
донесување и одобрување. Исто така, се овозможува подобрување
ративната ефикасност на владините институции и судството, при
е се унапредат: квалитетот на услугите кои министерствата ги
дуваат за граѓанскиот и за приватниот сектор, електронската
документи процесирани во секоја институција, намалувањето на
ивните трошоци, полесната достапност до информации, целосната
ција на предметите (во правосудството), брзото пребарување,
онското архивирање и зачувување.
својот пат до примачот, информацијата може да се пресретне,
ожде да се дешифрира. Шифрирањето и дешифрирањето бараат
тичка формула или алгоритам, чија цел е конвертирање на
ци (од шифриран во читлив формат). Клучот е единствен број
комбинира со текстот за да се произведе шифрирана порака или
ен сертификат. Во зависност од тоа дали клучот (за шифрирање
фрирање) е ист, постојат - криптографија со таен и криптографија
клуч.

Криптографија со таен клуч

нарекува уште и симетрична криптографија. Користи ист клуч
ирање и дешифрирање на пораките, т.е. испраќачот и примачот
ст клуч. Значи, испраќачот и примачот можат да шифрираат и
ираат пораки со ист клуч. За да има безбедна комуникација,
жора претходно да е безбедно испратен до примачот и испраќачот.
никација меѓу институциите е потребен различен клуч.
нацирањето на протокот на податоци во јавниот сектор треба да
услугите на граѓаните да им се доставуваат на ефикасен начин
целосно да се приспособени на нивните потреби. Процесот
ементација на **криптографија со таен клуч** за заштита на
ите во јавниот сектор е еден од клучните фактори со кои јавната
рација прераснува во институција која ќе им нуди квалитетни

услуги на граѓаните, имајќи можност да изберат како, кога и каде ќе им пристапат на услугите.

Исто така, користењето на тајниот клуч овозможува истите цели да се постигнат преку понуда на владините услуги преку call центри, веб-портали и СМС. Притоа граѓаните ќе имаат можност да ги добијат услугите преку каналот на комуникација, што тие го преферираат без да имаат потреба да контактираат со голем број на државни службеници.



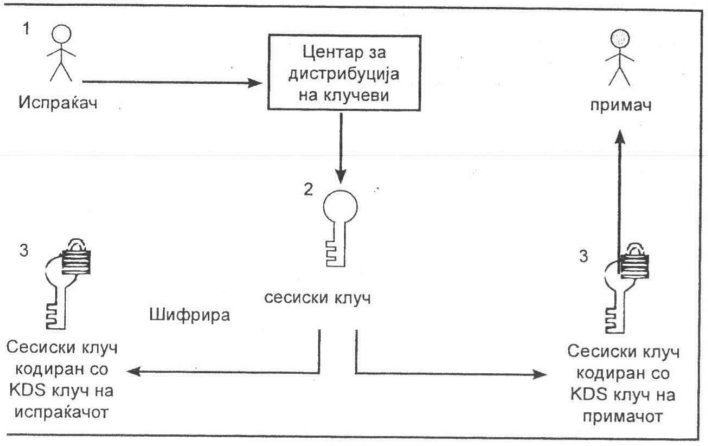
Сл.1 - Шифрирање/дешифрирање пораки со симетричен таен клуч

Алтернативен приод од оној за размена на клучеви е да се има централен авторитет за дистрибуција на клучеви (KDC). Во тој случај, дистрибутерот на клучеви за секоја сесија генерира различен клуч за секој пар корисници. Потоа секцискиот клуч се испраќа до испраќачот и примачот - шифриран со друг симетричен клуч кој се користи во комуникација меѓу централниот авторитет и корисникот.

Податокот е шифриран со првиот клуч, дешифриран со вториот клуч и повторно шифриран со третиот клуч.

Криптографија со јавен клуч

Главниот проблем кај криптографијата со таен клуч е: испраќачот и имачот треба да се договорат за тајниот клуч, без да дознае друг. Ако праќачот и примачот се наоѓаат на различни физички локации, тогаш е мора да најдат безбеден начин за нивна комуникација. Ако некој ог го дознае тајниот клуч, тогаш тој ќе може да ги чита и модифицира фрираните пораки кои го користат овој клуч.

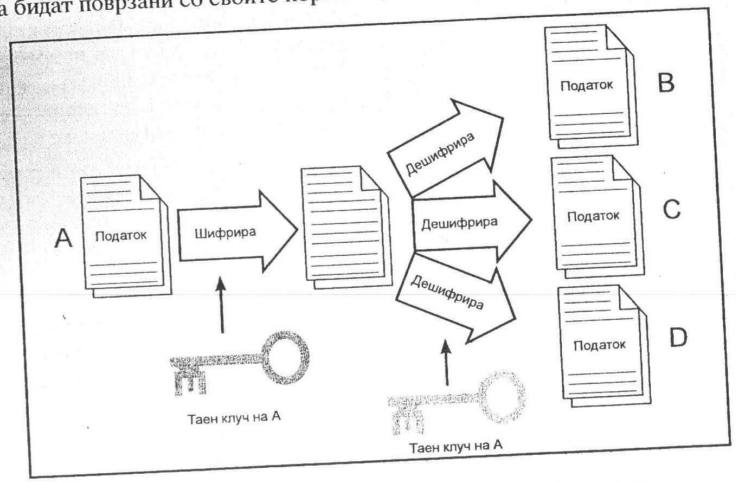


Сл. 2 - Пренос на секциски клучеви преку дистрибутивен центар

Генерирањето, преносот и меморирањето на клучот е наречено **ацирање на клуч**. Бидејќи сите клучеви во криптографијата со тајни ючеви мора да останат тајни, криптографијата со тајни клучеви често тешкотија со обезбедување на безбедно управување со клучевите, обно во отворени системи со голем број на корисници, како што се авните сервиси и институции. Со цел да се разрешат проблемите правување на клучот, истражувачи од Stanford развиле систем за тирање со јавен клуч. Овој систем е асиметричен.

Криптографијата со јавен клуч се користи за шифрирање и тални потписи. Во овој систем секој корисник има пар од клучеви, от е јавен а другиот е приватен клуч. Приватниот клуч е таен клуч знае само сопственикот на клучот. Јавниот клуч се дистрибуира рено. На овој начин потребата за споделување на тајната информација

е елиминирана, каква било комуникација го вклучува само јавниот клуч, додека тајниот клуч не се пренесува. Со овој систем е непотребно да им се верува на средствата за комуникација. Единствен услов е јавните клучеви да бидат поврзани со своите корисници на доверлив начин.



Сл. 3 - Шифрирање/дешифрирање порака со јавен клуч

Ако јавниот клуч се користи за шифрирање на пораката, таа може да се дешифрира само со приватниот клуч, и обратно. Секоја страна во комуникацијата има 2 клуча: јавен и приватен. Испраќачот го користи јавниот клуч на примачот за да ја шифрира пораката. Примачот ја дешифрира со својот приватен клуч. Не постои начин од јавниот клуч да се изведе приватниот клуч. Само корисникот за кој е наменета пораката ќе може да ја прочита.

Цел е преку веќе интегрираниот информативен систем во правосудството, јавната администрација или министерствата, предметите кои електронски им се распределуваат на државните службеници да бидат заштитени од неовластено користење и поседување, но и се избегнува субјективноста на човечкиот фактор при нивно доделување. Заштитата се прави во т.н. центри на податоци со цел да се поврзат различните сегменти во институцијата што ќе овозможи ефикасна и безбедна размена на податоци и извештаи. Овие активности воспоставуваат и развиваат модерна и ефикасна држава, каде главни сегменти се правосудството и

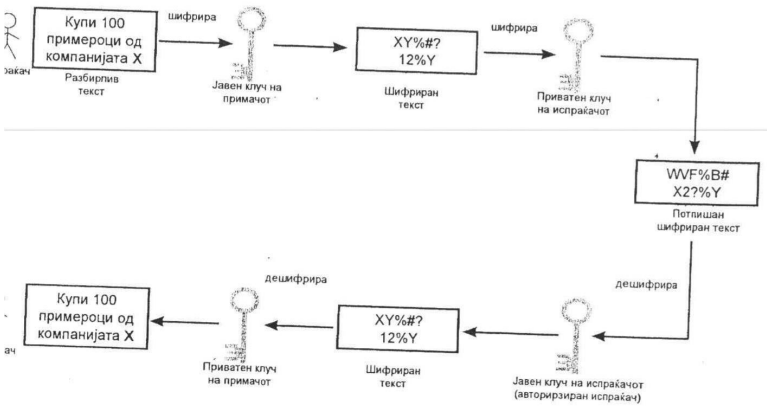
јавната администрација. Затоа, решенијата и системите на заштита треба да се во согласност со најдобрите европски стандарди, меѓу кои припаѓа примената на јавниот клуч.

За шифрирање на пораката може да се користат и јавниот и приватниот клуч. Ако корисникот ја шифрира пораката со јавниот клуч на институцијата, таа ја дешифрира со својот приватен клуч, но потребен е механизам за да се потврди идентитетот на корисникот. Обратно, ако пораката е шифрирана со приватен клуч на корисникот, а е дешифрирана со јавниот клуч на корисникот кој го има институцијата, тогаш може да се потврди идентитетот на корисникот.

RSA алгоритам

RSA е алгоритам за криптографија со јавен клуч. Тоа е првиот познат алгоритам кој е соодветен за дигитални потписи. Откривањето на овој алгоритам претставува голем напредок во криптографијата со јавни клучеви. RSA е широко употребуван, како во електронските комерцијални протоколи така и во владиниот сектор и правосудството. Поради тоа што алгоритам за криптографија со јавен клуч, тој вклучува јавен и приватен клуч. Клучевите на RSA алгоритамот се прикажани на сл. 4.

Сигурноста на овој алгоритам произлегува од фактот дека се користат многу големи прости броеви. Овој алгоритам, пред сè, се користи и дигитални потписи.



Сл. 4 - Идентификација на учесници во комуникација, алгоритам со јавен клуч

Дигитални потписи

Дигиталните потписи се креираат за да се надмине проблемот на автентичност на податоците, кои се дистрибуираат во информационен систем, каде како криптографска заштита се користи јавен клуч.

Испраќачот ја зема пораката и ја пропушта низ *хеш* (hash) функција, за да креира *хеш* вредност. *Хеш* функција може да биде едноставно собирање на сите единици во пораката, иако обично е многу покомплексно. *Хеш* вредноста е исто позната како дигитална порака. Постои мала веројатност дека две пораки ќе имаат иста *хеш* вредност. Ако тоа се случи настанува колизија. Потоа испраќачот го користи својот приватен клуч за шифрирање на *хеш* вредноста. Овој чекор креира дигитален потпис и го идентификува испраќачот. Оригиналната порака шифрирана со јавниот клуч на примачот, дигиталниот потпис и *хеш* функцијата се испраќаат на примачот.

Примачот на информацијата го користи јавниот клуч на испраќачот за дешифрирање на дигиталниот потпис за да добие дигитална порака. Потоа го користи сопствениот приватен клуч за дешифрирање на оригиналната порака. На крај, примачот ја применува *хеш* функцијата на оригиналната порака. Ако *хеш* на оригиналната порака се согласува со пораката вклучен во потписот, тогаш интегритетот на пораката е зачуван, односно таа не е изменета за време на преносот. Дигиталниот потпис се креира користејќи ја содржината на документот, така тој е различен за секој документ на корисникот.

Целта на користењето на дигиталниот потпис е да се идеализира заштитата на податоците, со што се овозможува целосна примена на законите од областа на електронското управување, при што се дава вистинска можност да се користат документите во електронска форма, исто како и пишаните документи.

Литература

Rosenfield L. (2008), "Information Architecture for the WWW", O'Reilly and Associates.

Elias M. (2006), "Electronic Commerce From Vision to Fulfillment – 3th edition", Prentice Hill.

Cormen T. Charles L. Ronald R. Clifford S. (2001), "Introduction to Algorithms - 2th edition", MIT Press and McGraw-Hill

Mark W. (1997), "How to use Internet", ZD Press.